Bijlage A Programma van Eisen – GRC systeem

Voor de gemeente Velsen is het belangrijk om grip te houden op informatiebeveiliging en privacy. Daarom willen we ondersteund worden door een systeem dat inzicht en overzicht biedt op de risico's, normen en maatregelen. Het systeem moet de spil vormen in het Information Security Management System (ISMS) en Privacy Management System (PMS) van de gemeente Velsen en in de toekomst mogelijk ook in andere risicobeheersingssystemen. In dit document beschrijven we de onze eisen voor het leveren, onderhouden en ondersteunen van een Governance, Risk and Compliance (GRC) systeem.

1. Functionele eisen

Nr.	Eis
1.1	De toepassing ondersteunt verschillende frameworks, waaronder maar niet beperkt tot, frameworks voor: • Privacy control, inclusief AVG borgingsproduct (IBD), ISO27701 en het Norea privacy control framework • Informatiebeveiliging, inclusief BIO, ISO27001, ISO27002 • Toetsingskaders, zoals Norea toetsingskaders: volwassenheidsmodel informatiebeveiliging, ENSIA en Wet politiegegevens. Minimaal dienen in de toepassing al frameworks aanwezig te zijn ter ondersteuning van het Information Security Management System (ISMS) en het Privacy Management System (PMS).
1.2	De toepassing biedt de mogelijkheid voor het afnemen van geactualiseerde frameworks en normenkaders (versiebeheer door leverancier).
1.3	De toepassing moet beschikken over contextgevoelige helpfunctie waarbij bij het oproepen van de helpfunctie direct informatie wordt getoond die relevant is voor de module en het onderdeel waaraan wordt gewerkt.
1.4	Het moet mogelijk zijn om bij beheersmaatregelen bewijs en/of toelichting toe te voegen in de vorm van een tekstveld en in de vorm van documenten.
1.5	Het moet mogelijk zijn om activiteiten t.b.v. beheersmaatregelen binnen de PDCA-cyclus te plannen en toe te wijzen aan een uitvoerder. Per activiteit moet de voortgang aangegeven kunnen worden als percentage of fasen (bijvoorbeeld niet gestart, gestart, review, afgerond).
1.6	Reviewers moeten rechten hebben om beheersmaatregelen of het bewijs voor het bestaan of de werking van beheersmaatregelen goed te keuren of af te keuren. Beheersmaatregelen moeten door de reviewer voorzien kunnen worden van commentaar in een specifiek veld voor de reviewer.
1.7	De toepassing moet het mogelijk maken om een self assessment uit te voeren voor geselecteerde frameworks en om (externe) audits uit te voeren voor geselecteerde frameworks. De toepassing ondersteunt dat hiertoe specifieke rechten gegeven kunnen worden.

1.8	Het moet mogelijk zijn om beheersmaatregelen(sets) in frameworks aan te passen of niet van toepassing te verklaren.
1.9	De toepassing moet in staat zijn een mapping aan te maken van controls/beheersmaatregelen over frameworks heen. Deze mapping moet ervoor zorgen dat identieke beheersmaatregelen uit verschillende frameworks, maar één keer hoeven te beantwoorden met acties, documentatie, bewijs, en commentaar.
1.10	Verschillende frameworks moeten in de toepassing geladen kunnen worden en naast elkaar gebruikt kunnen worden.
1.11	Bij een nieuwe versie van een framework dient informatie betreffende een bepaalde maatregel of onderdeel van het framework, zoals al bestaande documentatie, bewijs, commentaar en acties, behouden blijven en beschikbaar zijn in de nieuwe versie.
1.12	De toepassing dient frameworks met verschillende diepgang of opbouw te kunnen verwerken, waaronder maar niet beperkt tot bijvoorbeeld domeinen, hoofdnormen, subnormen, maatregelen en/of submaatregelen.
1.13	Binnen de toepassing dient het mogelijk te zijn om bij beheersmaatregelen zowel handreikingen op te nemen, als opmerkingen toe te voegen in een tekstveld.
1.14	De toepassing moet een operationeel risicomanagementsysteem bevatten waarmee risico's ten minste kunnen worden gekoppeld aan: • Een organisatieonderdeel, • Een bedrijfsproces, • Een bedrijfsmiddel • Eén of meerdere beheersmaatregelen • Eén of meerdere acties
1.15	De toepassing moet in staat zijn om per organisatieonderdeel, bedrijfsproces of bedrijfsmiddel een risicoregister samen te stellen.
1.16	Binnen de toepassing dient het mogelijk te zijn om bij risico's in het risicoregister documenten toe te voegen, waaronder maar niet beperkt tot risicoanalyses en beschrijvingen van maatregelen.
1.17	Het moet mogelijk zijn om risico's met bijbehorende beheersingsmaatregelen vanuit een bestand (CSV-formaat) te importeren in het risicoregister van de GRC-applicatie.
1.18	Binnen de toepassing dient het mogelijk te zijn om van elk afzonderlijk risico een risicoscore te berekenen door de kans op het optreden van het risico te vermenigvuldigen met de impact van het risico.
1.19	Risico's moeten opnieuw beoordeeld kunnen worden om het risico-overzicht te actualiseren.
1.20	Binnen de toepassing dient het mogelijk te zijn om risico's aan meerdere normen te koppelen en om meerdere beheersmaatregelen aan een risico te koppelen.
1.21	Binnen de toepassing dient het mogelijk te zijn voor geautoriseerde gebruikers om een prioriteit aan een taak te geven en te wijzigen. De toepassing heeft ten minste de mogelijkheid de prioriteiten laag en hoog toe te kunnen kennen.

1.22	Het moet mogelijk zijn om een of meerdere taken per risico toe te wijzen.
1.24	De toepassing dient bij het risicomanagement de mogelijkheid te hebben om aan te geven wat het restrisico is dat overblijft na de genomen beheersmaatregelen.
1.25	De toepassing dient het mogelijk te maken om in formulieren te kunnen filteren op wat getoond wordt en wat niet getoond wordt.
1.26	Het moet mogelijk zijn om taken aan te maken en toe te wijzen aan actiehouders.
1.27	Taken moeten via workflow uitgezet kunnen worden. Hierbij moeten notificaties en rappels via e-mail verstuurd kunnen worden. Bij voorkeur gebeurt dit wanneer de afhandeldatum nadert en is dit instelbaar.
1.28	Bij taken dient een einddatum geselecteerd te kunnen worden.
1.29	Uitzetten van wederkerende taken moet ondersteund worden (audit, controle en implementatie taken).
1.30	De toepassing dient GAP-analyses te ondersteunen, bijvoorbeeld bij het rapporteren over naleving van de BIO waarbij de GAP tussen de behaalde score en de gewenste score gegeven moet kunnen worden en waarbij de GAP gegeven moet worden welke beheersmaatregelen nog niet geheel in werking zijn.
1.31	De GRC-applicatie moet de mogelijkheid bieden om risico's en maatregelen te koppelen aan verschillende organisatieonderdelen.
1.32	Binnen de toepassing moet het mogelijk zijn om een register van verwerkingen van persoonsgegevens op te bouwen en te onderhouden. De GRC-applicatie biedt alle functionaliteit voor een register van verwerkingen waarmee de gemeente Velsen de Algemene Verordening Gegevensbescherming kan naleven.

2. Eisen t.a.v. authenticatie

Nr.	Eis
2.1	De toepassing biedt een autorisatiemechanisme waarmee de volgende rollen onderscheiden kunnen worden: • Beheerder: kan andere gebruikers rechten geven tot specifieke onderdelen van de toepassing. • Hoofdgebruiker: kan frameworks aanpassen en functionaliteiten toevoegen/weglaten en kan de GRC-applicatie zelf gebruiken. • Gebruiker: kan voor een specifieke taak input geven. • Review: kan afgeronde taken bekijken en daar een oordeel bij geven.
2.2	Toegang tot de toepassing is gebaseerd op role based access.
2.3	Elke gebruiker mag enkel die gegevens zien waartoe ze zelf geautoriseerd zijn.

3. Eisen t.a.v. implementatie

Nr.	Eis
3.1	De GRC-applicatie dient de migratie vanuit een andere GRC-applicatie te ondersteunen. Dit geldt voor: • het importeren van frameworks, • het importeren van een risico register, • het importeren van historische gegevens.
3.2	Inschrijver zorgt ervoor dat bij ingebruikname van de toepassing door de opdrachtgever een handleiding beschikbaar is over het gebruik van de volledige functionaliteit van de toepassing.
3.3	Inschrijver dient trainingen in het gebruik van de applicatie te kunnen geven. De trainingen dienen toegespitst te zijn op het type gebruiker.

4. Eisen t.a.v. rapportage en ISMS-documenten

Nr.	Eis
4.1	Met de GRC-applicatie moeten tenminste de volgende rapportages kunnen worden aangemaakt: • gedetailleerde rapportage over de voortgang (van de taken in, bijvoorbeeld een jaarplan), • managementrapportage over de voortgang (bijvoorbeeld van openstaande taken, afgeronde taken, percentages van taken die uitgevoerd zijn), bij voorkeur met de mogelijkheid tot selectie van onderdelen. • rapportage over uitgevoerde metingen en GAP-analyses op normenkaders.
4.2	Met de GRC-applicatie moeten tenminste de volgende ISMS-documenten kunnen worden aangemaakt: • jaarplan met prioriteitsstelling na meting en overzicht taken met planning en verantwoordelijk organisatieonderdeel, • verklaring van toepasselijkheid.
4.3	De GRC-applicatie moet rapportages en ISMS-documenten kunnen exporteren in minimaal MS-Word-formaat en bij voorkeur ook in MS-Excel-formaat.

5. Eisen t.a.v. dienstverlening

Nr.	Eis
5.1	Inschrijver ondersteunt bij het importeren van data uit andere ISMS- en GRC-toepassingen.
5.2	Inschrijver levert op verzoek van Opdrachtgever ondersteuning bij het inlezen van frameworks.

6. Eisen t.a.v. SaaS

Nr.	Eis
6.1	De GRC-applicatie wordt volledig als een online (SaaS) dienst aangeboden. De gebruiker benadert de software over het internet bij de aanbieder van de dienst.
6.2	De GRC-applicatie werkt vanuit de meest gebruikte, gangbare browsers, waaronder maar niet beperkt tot Microsoft Edge en Google Chrome.
6.3	De GRC-applicatie werkt in de browser zonder add-ons, plug-ins of andere extra software aan de kant van de gebruiker.
6.4	De aanbieder verzorgt onder meer het technisch beheer, het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates.
6.5	De GRC-applicatie wordt aangeboden in het Nederlands en, bij voorkeur ook Engels, waarbij een gebruiker de gewenste taal kan selecteren.
6.6	De data van de opdrachtgever is gescheiden van de data van andere klanten.
6.7	De GRC-applicatie moet een veilige audittrail logging bevatten met daarin minimaal: • Wie heeft een activiteit uitgevoerd. • Welke activiteit is uitgevoerd (create, update, delete). • In welk onderdeel is de activiteit uitgevoerd. • Wanneer is de activiteit uitgevoerd.
6.8	Data is tijdens transport en in opslag beveiligd via encryptie.
6.9	De oplossing dient inloggen via MFA te ondersteunen.
6.10	Inschrijver heeft een geldige en op de gehele dienstverlening toepasselijke certificering ISO27001 of gelijkwaardig. Inschrijver toont dit na gunning aan de opdrachtgever aan door het overleggen van het certificaat met verklaring van toepasselijkheid en scope-beschrijving.

6.11	Opdrachtnemer leeft de AVG na wat betreft datalekken, privacyvraagstukken en de bescherming van persoonsgegevens en heeft, bij voorkeur, een DPIA op de applicatie uitgevoerd.
6.12	De GRC-applicatie dient inloggen via de Azure AD van de opdrachtgever te ondersteunen.
6.13	Inschrijver zorgt dat gegevens, ook in geval van bijvoorbeeld een incident, niet verloren gaan, dan wel dat ze met maximaal 1 dag verlies hersteld kunnen worden.
6.14	Inschrijver ondersteunt de opdrachtgever in het geval die een restore willen doen van eerdere data door het terugzetten van data uit een back-up.
6.15	De inschrijver voert jaarlijks een restore test om te controleren of de back-up en restore van de GRC-applicatie betrouwbaar en volledig is en deelt de resultaten hiervan met Opdrachtgever.
6.16	Privacy en security by design is toegepast bij ontwerp en (door)ontwikkeling van de oplossing.
6.17	Alle gegevens worden opgeslagen binnen de grenzen van de Europees Economische Ruimte (EER).
6.18	Alle intellectuele eigendomsrechten op ingevoerde data en documentatie blijven te allen tijde eigendom van de opdrachtgever.
6.19	Beschikbaarheid van de toepassing moet minimaal gelijk zijn aan 99% per kalendermaand binnen het afgesproken service window. Hierbij wordt de beschikbaarheid berekend met de volgende formule: *(([de som van de minuten binnen het service window per kalendermaand] minus [de som van de minuten van niet-beschikbaarheid binnen het service windows per kalendermaand]) gedeeld door ([de som van de minuten binnen het service window per kalendermaand])) x 100%.*
6.20	Page load time maximaal 7 seconden (pagina performance).
6.21	Inschrijver heeft een helpdesk voor ondersteuning voor alle gebruikers van de toepassing in zowel de Nederlandse als de Engelse taal. De helpdeskondersteuning is bereikbaar van maandag tot en met vrijdag van 08.00 tot en met 17.00 CET (Central European Time), met uitzondering van de in Nederland algemeen erkende feestdagen.
6.22	Onderhoudswerkzaamheden aan de toepassing door de leverancier die leiden tot een beperking in de beschikbaarheid van de toepassing vinden buiten het Service Window plaats.
6.23	Geplande uitval van de toepassing wordt minimaal twee werkdagen vooraf aan de uitval gemeld aan de gebruikers van de toepassing.
6.24	Inschrijver maakt een roadmap voor de (door)ontwikkeling van de applicatie en bespreekt deze ten minste twee keer per jaar met opdrachtgever.

6.25	Inschrijver biedt de opdrachtgever de mogelijkheid om wensen in te dienen voor functionaliteit van de toepassing. Bij voorkeur worden deze wensen besproken en geprioriteerd voor realisatie in een gebruikersgroep waarin ook klanten vertegenwoordigd zijn.
6.26	Na opdrachtverstrekking ondertekent de opdrachtnemer de, door de opdrachtgever opgestelde, verwerkersovereenkomst voordat er tot de daadwerkelijke verwerking van persoonsgegevens wordt overgegaan. De verwerkersovereenkomst is gebaseerd op het VNG-model. In samenspraak tussen opdrachtgever en opdrachtnemer kunnen wijzigingen worden aangebracht die specifiek voor de opdracht van kracht zijn.

7. Eisen t.a.v. Contractbeëindiging

Nr.	Eis
7.1	Inschrijver zal na het beëindigen van de overeenkomst en het teruggeven van de data aan de opdrachtgever, de data van de systemen onder beheer van Inschrijver verwijderen nadat de opdrachtgever hiertoe akkoord heeft gegeven. Voor het verwijderen van de data zullen geen additionele kosten in rekening worden gebracht.
7.2	Bij beëindiging van de overeenkomst wordt alle gestructureerde data en documenten opgeslagen is de GRC-applicatie teruggegeven aan de opdrachtgever. Gestructureerde data worden in gedenormaliseerde vorm met CSV-bestanden aan de instellingen ter beschikking gesteld. Gekoppelde documenten in hun originele formaat. Voor het beschikbaar stellen van de data zullen geen additionele kosten in rekening worden gebracht.
7.3	Inschrijver blijft tijdens de periode totdat de beëindiging van de overeenkomst een feit is de dienstverlening leveren conform de gemaakte vereisten en afspraken.
7.4	Inschrijver waarschuwt en adviseert in de bespreking over of de voorbereiding van de contractbeëindiging tijdig over noodzakelijke werkzaamheden en maatregelen voor de contractbeëindiging.